Stimmabgabeprozess

Initiale Einrichtung

1. WahlleiterIn authentifiziert sich mit einem nur der oder dem WahlleiterIn bekannten Passwort. Alle Aktionen der Wahlleiterin werden vom Server nur ausgeführt wenn dieses Passwort das für die Serverinstanz konfigurierte ist
2. WahlleiterIn importiert den Basisstamm an Daten für die betreffende Wahl aus einer CSV Datei (Kandidaten, Parteien, etc)
3. WahlleiterIn sperrt die (statistische-) Auswertung der betreffenden Wahl um jegliche Wahlbeeinflussung durch vorläufige Auswertungen ausschließen zu können über einen Slider in der UI
4. WahlleiterIn generiert ein PDF über einen Button in der UI, welches die Zugangstokens für die WahlhelferInnen enthält. Da aufgrund von Datenmangel keine Stimmbezirke im System modelliert sind, gelten diese Zugangstoken für einen ganzen Stimmkreis. Dies hat jedoch keinen technischen Grund und das System funktioniert identisch mit fein granulareren Zugangsberechtigungen, e.g. auf Stimmbezirksebene oder sogar für jede(n) einzelne(n) WahlhelferInn
5. WahlleiterIn übermittelt die Zugangstoken den berechtigten Personen über einen geschützten Kanal.
6. Berechtigte Person fährt Wahlkabinen hoch und nutzt das von der oder dem WahlleiterIn zugesandte Token um die Wahlkabinen einmalig zu authorisieren.

Wahl

1. WählerIn betritt Wahllokal und wird von WahlhelferInn einer Identitätsprüfung unterzogen (Personalausweis, Reisepass)
2. WahlhelferInn gibt eine nicht besetzte Wahlkabine über einen Slider in der UI frei und weist der oder dem WählerIn die entsprechende Wahlkabine zu
3. WählerInn betritt Wahlkabine und wird ab diesem Punkt von der UI durch den gesamten Stimmabgabeprozess geleitet
4. Nach der Stimmabgabe entzieht der Server der Wahlkabine die Freigabe und verhindert somit eine mehrfache Abgabe
5. WählerIn verlässt das Wahllokal

Sicherheit

- Die Mehrfache Stimmabgabe wird dadurch verhindert, dass ein(e) WahlhelferIn je die Wahlkabine zur Stimmabgabe freigeben muss, und das System der Wahlkabine nach einer Stimmabgabe diese Freigabe wieder entzieht
- Nicht authorisierte Personen können keine Stimme abgeben, da hierzu ein autorisierter Wahlkabinentoken sowie die Freigabe für diesen Token erworben werden muss. Da nur der Wahlleiter sein Passwort kennt, würde eine nichtautorisierte Person Einfluss auf diesen haben müssen. Dies ist auch im bestehendem analogen System. De facto bleiben als einzige neue Angriffsfläche die Authorisierungstoken der Stimmkreise (bzw. Sofern in einem echten System bessere Daten zur Verfügung stehen, die der Stimmbezirke oder sogar pro Wahllokal die des oder der WahllokalleiterIn). Da diese Token aber gut gehütet und nur geschützt versendet werden, bedarf es eines oder einer nicht vertrauenswürdigen WahlhelferIn damit

das zum Problem wird. Dies ist auch im bereits existierenden analogen System fatal. Im Vorteil zum Analogen System kann jede Aktion haar genau mit dem dazu gehörigen Token gelogged werden.
- SQL-Injections sind kein Problem da nur prepared statements verwendet werden
- Die Serverschnittstelle ist eine von Apollo Server bereitgestellte GraphQL Schnittstelle, welche aufgrund der Industrieunterstützung und dem breiten Produktiveinsatz als sicher angesehen werden kann.